

**Statement of Objectives (SOO)**  
**Defense Manpower Data Center (DMDC)**  
**Identity & Credential Enterprise Solution & Services (ICES2)**

The Contractor shall provide the materials and services required support the implementation of the Identity & Credential Enterprise Solution ICES<sup>2</sup> Application in accordance with the contractor's Performance Work Statement (PWS). The contractor's PWS will be incorporated at task order award. The below Statement of Objectives (SOO) will be deleted at task order award.

**1.0 INTRODUCTION/ BACKGROUND:**

- a. The historical approach and legacy solution:
  - i. In 2000-2004, DMDC developed a solution called the Real-time Automated Personnel Identification System (RAPIDS), which over time became the system that issues the Common Access Card (CAC) and the Uniformed Services Identification (USID) card.
  - ii. In late 2004-2006, DMDC incorporated aspects of the HSPD-12 mandate and the FIPS 201 standard into RAPIDS. The CAC is Department of Defense (DoD's) implementation of the Federal Personal Identity Verification (PIV) card mandated by HSPD-12 and FIPS 201.
  - iii. **Appendix B** - Legacy Overview; **Appendix C** – Current capabilities; **Appendix C1** - Next Generation Credential PIN Reset Functional Specifications; **Appendix X1** - Legacy COTS hardware components; and **Appendix X2** - Legacy RAPIDS COTS software components).
- b. The new approach:
  - i. Since 2004, significant innovation in the commercial marketplace of Commercial Off the Shelf (COTS) solutions has emerged that complies with NIST 800-63, FIPS 201 and its objectives, and supports a robust set of commercial credentialing processes. These COTS solutions have the capability to perform the DMDC mission and offer a wide range of new initiatives and capabilities to augment the fully standards-compliant mission of DoD identity and credentialing capabilities.
  - ii. Centers on a modular, severable, highly scalable, fault-tolerant, COTS architecture. DMDC requires a non-proprietary solution for managing its identity management and credentialing mission. This includes development, sustainment, and maintenance.
  - iii. **Appendix A** - To Be Overview

**2.0 OBJECTIVE:**

The objective of this task order is to utilize the Agile development process to establish the Identity & Credential Enterprise Solution & Services (ICES<sup>2</sup>) platform. This effort shall establish innovative solutions through reusable modules/services which can be integrated together to deliver identity and credential capabilities. The purpose of the service will be to provide the DoD with an enterprise solution to support identity, affiliation, and credential management. The new service will replace all critical and major business processes supported today by the legacy Real-time Automated Personnel Identification

System (RAPIDS) Suite.

**a. Overall Program Objectives:**

- Initial system design, implementation, and training
- System configuration to support business processes
- Integration
- Sustainment and maintenance of the system
- Prototype future technologies, solutions, and capabilities

The program objectives do NOT include:

- Operating the system/application in the field
- Training end users on new system

**b. System Objectives:**

- a. Provide a reusable, modular architecture with severability of individual components, including decoupling services to reduce dependencies.
- b. Provide a phased approach for design, development, integration, and deployment (including any pilots if applicable).
- c. Provide a rollout plan that ensures existing ID cards are supported and can continue to be used until all ID cards have been replaced by attrition with the new solution.
- d. Follow DMDC development and release standards including a governance process for approval of innovative processes, solutions, technology, and architecture in accordance with **Appendix D – Software Development Life Cycle (SDLC)**.
- e. Design the system for maximum interoperability across all components and offices to ensure flexibility in leveraging system for future applications.
- f. Approach the system design as an “off-the-shelf” (e.g., COTS, open source) manner as much as possible with focus on preventing or minimizing system customization, in accordance with DoD CIO Memo on Open Source Software (<https://dodcio.defense.gov/Portals/0/Documents/Library/SoftwareDev-OpenSource.pdf>).

GOTS will be considered where “off-the-shelf” cannot meet DoD needs. Examples include:

- i. COTS licenses and maintenance (product capable of integration and operations by a third-party or the government)
- ii. COTS Enrollment Software Licenses and maintenance (product capable of integration and operations by a third-party or the government)
- iii. COTS hardware (HW) (workstations, kiosks) and maintenance (product capable of integration and operations by a third-party or the government)
- iv. COTS HW (enrollment and issuance peripherals) and maintenance (product capable of integration and operations by a third-party or the government)
- v. Professional services from COTS providers
- vi. All GOTS development and integration activities under this contract is ownership of the government; integration and configuration of COTS cannot be made proprietary
- vii. The solution must be articulate of licenses for COTS and/or third-party components
- g. Ensure product compatibility and integration
- h. Deliver cloud native/agnostic capabilities, including redundancy and fault tolerance

- i. Identify whether cloud hosting location is contractor or government; production deployment must be to DoD-approved and managed, accreditable cloud environment (e.g., OCI, AWS)
- j. Fully support/enable COOP/disaster recovery (DR) practices
- k. Adhere to DMDC standards for data store interfaces/updates
- l. Leverage open data standards and interfaces
- m. Adhere to Government owned data and engineering specifications
- n. Provide capacity planning to predict or anticipate future growth
- o. Adhere to Agile project guidelines and specifications
- p. Adhere to relevant NIST Special Publications and DoD policies (e.g., SP 800 175B, SP 800-131A)
- q. Enable elastic capacity (expand/contract) resources in an autonomic manner in real time
- r. Use approved and acceptable key management to enable secure encoding of Common Access Cards (CACs) (legacy uses Hardware Security Modules (HSMs))
- s. Reduce card token waste during production outages.
- t. Provide live warning capabilities (e.g., alert and status to users before actual card issuance).
- u. Proactively identify changes to existing and draft Federal and DoD policy necessary to support deployment and continuous improvement of new solutions
- v. Incorporate tools to enable easily monitoring the solution and service, including collecting, searching, troubleshooting, and analyzing system metrics and logs to ensure developers and operational team have full visibility into entire system
- w. Enable a fault tolerant architecture design to ensure system anticipates failure and continue operational rather than failing completely when some part of the components fails. System should self-recover, self-stabilize from production issues rather than complete restart of the system manually.
- x. Provide support for planning and communications on deployment and production rollout.
- y. Provide support DoD Risk Management Framework (RMF) and maintain an Authority to Operate (ATO) (**Appendix E**)
- z. Minimize/reduce fielded hardware footprint and responsibilities for centrally managing workstations, and encourage mobility

### 3.0 SCOPE:

In support of its mission, DMDC needs contractor support services to develop and deliver a FIPS 201-3-compliant solution for managing identities, affiliation, and credentials, including ability to scale to support the DoD's current and evolving requirements (e.g., post-quantum algorithms, other credential types and form factors).

### 3.1 TECHNICAL OVERVIEW

#### a. Technical Environment

The platform will contain Sensitive But Unclassified (SBU) and Personally Identifiable Information (PII). No classified information will be contained in these systems. Federal Information Processing Standard (FIPS) 199 classification is Moderate for Availability, Moderate for Integrity, and Moderate for confidentiality. Reference **Appendix B and C** for legacy RAPIDS Suite information and capabilities.

#### b. Stakeholders

For the completion of this task, DMDC will provide access to the following stakeholders:

**Government Technical Lead/Product Owner/Program Manager:**

- Manages and communicates with the stakeholder community,
- Makes business decisions rapidly and set priorities,
- Participates in iterative planning sessions and will remove obstacles to project success.

**DMDC Contracting Officer's Representative (COR):**

- Responsible for approving deliverables,
- Manages the Quality Assurance Surveillance Plan (QASP),
- Evaluates performance and manages schedule according to the submitted Performance Work Statement (PWS) and approved project schedule.

#### **4. REQUIRED TASKS**

**a. Task 1: Initial System Configuration and Implementation**

The contractor shall provide secure, stable, reliable, standards-compliant, modular/reusable services-based, "off-the-shelf" collaboration solutions to deliver on the DoD's identity and credentialing mission. (**Appendix C - Current RAPIDS Suite Capabilities**)

- i. The solution must adhere to DoD regulations and requirements for "off-the-shelf" software and GOTS. The solution must adhere to DoD regulations and requirements for cybersecurity, in accordance with DFARS.
- ii. The solution shall consider credentialing standards and requirements, to allow flexibility in process and approach based on the requirements for the credential (e.g., DoD Common Access Card (CAC) is bound by requirements driven by Federal guidance whereas Uniformed Services ID (USID) cards are not).

**b. Task 2: Enterprise Identity System Design and Implementation**

The contractor shall design and implement the basic system features to deliver standards-compliant identity and credentialing solution, including the following (**Appendix A**):

- i. Identity management solution to allow trained/approved users to capture and maintain/update biometrics, biographic information, and supporting identity documents for an individual.
- ii. Affiliation management solution to allow trained/approved users to capture and maintain/update affiliation to the DoD (including termination of an affiliation).
- iii. Credential management solution to allow trained/approved users to create, maintain, and terminate DoD credentials
- iv. Inventory management solution to manage cardstock and consumables inventory from central location to/from DoD locations worldwide
- v. Personal Identification Number (PIN) Management
- vi. Self-Service capabilities
- vii. Mobile ID Card
- viii. Appropriate integration of solutions for smooth user experience and usability.



- ix. Transition and cut-over approach, to transition from legacy solution to ICEs<sup>2</sup>

**c. Task 3: Integration**

The Enterprise Identity System shall be integrated with DMDC's data repositories and relevant systems including the following:

- i. Integration with DMDC Personnel Data Repository (PDR) and other data repositories, including access to appropriate data.
- ii. Integration with DMDC products and capabilities.
- iii. Integration with Identity, Governance, Administration (IGA) – Enterprise Monitoring and Management of Accounts (EMMA) or other designated ICAM solution (e.g. DISA Identity Credential and Access Management) ICAM solution) for role/user management.
  - a. EMMA is a DMDC-wide framework for implementing and managing application security. Using the family of EMMA Products, applications are able to construct and define a hierarchy for application access using the EMMA Admin Tool and use EMMA web for provisioning and managing their hierarchy of users authenticated to specified roles.
- iv. Integration with Identity Resolution/Probabilistic Search

**d. Task 4: Sustainment and maintenance of the system**

The contractor shall provide all aspects of support to sustain and maintain the system.

- i. Enable 24x7x365 operations.
- ii. Sustain and maintain ICEs<sup>2</sup>.
- iii. Comply with DoD technology, security, and cybersecurity standards., including support to Risk Management Framework (RMF) and maintaining an Authority to Operate (ATO).

**e. Task 5: Review of new policies and cutting-edge technologies**

The contractor shall provide review of new and draft policies/laws and recommendations for new technologies to enable the DoD identity and credentialing mission.

- i. Review Federal and DoD-level policies and requirements
  - a. Review draft Federal and DoD-level laws and policies during informal and formal review periods to confirm impact to DMDC capabilities and provide recommendations for edits/changes.
  - b. Review new Federal and DoD-level laws and policies to confirm impact to DMDC capabilities, including LOE and timeline for implementation.
  - c. Examples include FIPS 201 and other NIST Special Publications, Executive Orders, Federal Memorandums, and NDAA requirements impacting identity or credentialing, as well as DoD policies and requirements.
- ii. Provide semi-annual report on industry ICAM trends, including new technologies and processes. Recommend prototypes and pilots, including supporting business case analysis.

**f. Task 6: Enhancements to the developed capability**

The contractor shall provide their process for submitting future enhancements and improvements to the developed capability. The process shall include requesting prototypes to be developed and

piloted for future technologies, enhancements, solutions, and capabilities.

**g. Task 7: Sustain and Maintain CAC PIN RESET (CPR)**

The contractor shall sustain and maintain the CPR. (Reference Appendix A).

**5. CONSTRAINTS**

DMDC follows DoD and DMDC processes for software development, including the DMDC Service Delivery Model (SDM) and the Software Development Life Cycle (SDLC). The contractor should propose, with detail, innovative processes, architectures, solutions, and technologies to meet the Statement of Objectives. Processes, architectures, solutions, and technologies that are not already approved by DoD must go through the DMDC approval process.

**6. DELIVERABLES**

The contractor shall ensure proper control and coordination of all deliverables as proposed in the PWS to ensure they are on time.

Inspection and acceptance of deliverables procedures are as follows, unless modified in this TO:

- The Government will provide written acceptance, comments, and/or change requests, if any, within ten (10) calendar days from receipt by the Government, of all required Contract deliverables unless a situation arises that would require a longer reasonable review time, such as an additional five calendar days, without being considered a Government delay. If such situations occur, the Government will notify the contractor as to the change in the review time.
- Upon receipt of the Government comments, the Contractor shall have five (5) calendar days to rectify the situation and re-submit the contract deliverable(s) if it is not a "draft" deliverable. If it is a "draft" deliverable, the Contractor shall rectify the situation before the next scheduled submission of this deliverable(s). If the Government is still not satisfied with the deliverable after three recertification attempts, the deliverable will be considered unacceptable.

**7. CONTRACT ADMINISTRATION DATA**

**7.1 Place of Performance**

The primary place of work shall be at the government facility as designated. The test and development lab will be used for this work. Contractor employees may be required to work at home, another approved activity within the local travel area, or at the contractor's facility in cases of unforeseen conditions or contingencies (e.g., weather events). The contractor shall submit a plan for the contractors proposal to work off site for approval by the COR.

**7.2 Period of Performance**

The period of performance for this task order is anticipated to be a base period of one (1) year, with five (5) one-year option periods

The Government shall have the unilateral right to exercise option periods in accordance with FAR Clause 52.217-9 Option to Extend the Term of the Contract:

- a. The government may extend the term of this contract by written notice to the contractor within thirty (30) calendar days before the contract expires; provided that the government gives the contractor a preliminary written notice of its intent to extend at least sixty (60) calendar days before the contract expires. The preliminary notice does not commit the government to an extension
- b. If the government exercises an option, the extended contract shall be considered to include this option clause
- c. The total duration of this contract, including the exercise of any options under this clause, shall not exceed seventy-two (72) months; with the exception of any potential bridge of the contract for an emergency continuance of contract performance to be awarded for the benefit of the Government

## **7.5 Government Point of Contacts**

### **Client Contracting Officer's Representative (COR)** **TBD**

#### **GSA Contracting Officer**

Eileen Flanigan  
GSA Federal Acquisition Service (Mid-Atlantic Region)  
Acquisition Operations Division (3QSB)  
100 S Independence Mall W  
Philadelphia, PA 19106-2320  
Voice: 215-446-5816  
eileen.flanigan@gsa.gov

#### **GSA Contract Specialist (CS)**

David Roberts  
GSA Federal Acquisition Service (Mid-Atlantic Region)  
Acquisition Operations Division (3QSBB)  
100 S Independence Mall W  
Philadelphia, PA 19106-2320  
Voice: (b) (6)  
david.a.roberts@gsa.gov

#### **GSA Project Manager/Contracting Officer's Representative (COR)**

Carol Carpenter  
GSA Federal Acquisition Service (Mid-Atlantic Region)  
Assisted Acquisition Service (3QFAA)  
100 S Independence Mall W  
Philadelphia, PA 19106-2320  
Voice: (b) (6)  
Carol.Carpenter@gsa.gov

## **7.6 Travel**

Travel is required under this contract. All Travel shall be approved in writing by the COR in advance of any costs being incurred by the contractor. All travel must be in accordance with the Joint Federal Travel Regulation.

Exact locations and frequency are unknown at this time. Specific locations, dates and personnel required, etc., shall be identified by DMDC during task performance. It is anticipated that trips will include travel to attend meetings and to support performance.

The Not-To-Exceed dollar value established for Travel is \$25,000.00 for the base period and option period 1, and \$5,000.00 for each additional optional period. This Travel ceiling shall not be exceeded without the advanced written approval of the GSA Contracting Officer.

All travel shall be pre-approved by the DMDC Project Manager and fully coordinated with the DMDC COR prior to conducting the travel to ensure that funding and approvals are obtained before incurring any travel costs. Reimbursement shall include full travel costs and per diem reimbursement consistent with the Federal Travel Regulations, and reimbursement of general and administrative expense, as appropriate. Where feasible, the contractor will use teleconferencing and electronic media transfers of data as much as possible to limit travel costs. The contractor will seek the least expensive form of travel as is practical to the fulfillment of the performance of the task order.

In accordance with FAR 31.205-46, travel costs are to be reimbursed at rates not to exceed the maximum locality per diem rates (the combination of lodging, meals and incidentals) in effect at the time of travel, as set forth in the Federal Travel Regulations, Joint Travel Regulation and Standards Regulations, Section 925, as applicable. All air travel must be booked on American flagged carriers, unless otherwise directed by the Contracting Officer. All invoices for travel reimbursement shall be accompanied by supporting receipts.

## **7.7 Other Direct Costs (ODC)**

The Government may require the Contractor to purchase ODCs that are an ancillary and necessary part of the solution under this Contract. Such Non-travel ODCs shall be integral and necessary to the overall Contract performance. General-purpose items required for the conduct of the Contractor's normal business operations will not be considered allowable ODCs in the performance of work under this Contract. Requirements may be identified during performance by the Government or the Contractor.

Prior to any purchase, the contractor shall obtain the GSA CO's written approval. The Contractor shall include the following in any request for ODC purchases: the purpose, description of specific items, estimated cost, cost comparison and copies of three (3) quotes to show competitive basis for fair and reasonable price determination, and rationale. The Contractor shall not make any purchases without a written approval from the client representative and GSA CO. All Non-travel ODC purchase requests must be routed through the client representative and GSA COR for GSA CO's approval prior to incurring costs. Emails sent by the GSA Contract Specialist providing CO approval are authorized.

The contractor shall purchase hardware and software necessary for development of the prototype up to the full operational capability (FOC).

Federal contracting laws and regulations apply to all Contractor open market purchases under this TO. Prices must be determined fair and reasonable from competitive sources and are subject to Government audit. The Contractor shall maintain records documenting competitive sourcing, in strict compliance with the competition requirements set forth in the Federal Acquisition Regulation (FAR), for all ODC purchases.



The Contractor shall provide copies of all such documentation upon request from the Government to verify that the Contractor complied with the competition requirements set forth in the FAR. The Contractor shall only be allowed to apply indirect rates to ODC costs after award if such application is consistent with their successful price proposal and DCAA recommendations. No profit or fee shall be permitted on ODCs.

All ODCs purchased under this contract shall become the property of the Federal Government. If the Contractor acquires hardware/software maintenance support, all licenses and/or contractual rights to receive title shall be turned over to the Government upon completion of the contract. The Government's liability to reimburse the Contractor for costs incurred from the acquisition of hardware/software maintenance support shall be limited to costs incurred during the period of the order.

#### **7.8 Government Furnished Equipment (GFE)**

The Government will provide computer and software resources for personnel designated as on site. The contractor has the primary responsibility for exercising reasonable care and control of GFE in its possession, or usage. Responsibility for reasonable care and control of GFE provided under the call order in the possession of a subcontractor remains with the prime contractor. The contractor may be liable for damages, shortages of GFE when it is disclosed that the equipment is lost, damaged, or destroyed. GFE must be used only for the purposes set forth in this call order.

Upon request of the Government, all Government furnished items shall be returned to the Government. All equipment or items furnished to the contractor shall be surveyed and a GFE/GFI list report shall be delivered to the COR at end of the call order.

#### **7.9 Government Furnished Information (GFI)**

The Government will provide the following information: access to relevant Government organizations, information and documentation, manuals, texts, briefs, and associated materials when required and available. Access will be granted to classified networks under the guidance of the appropriate Government Security Manager.

#### **7.10 Key Personnel**

Key personnel proposed shall include at a minimum a Program Manager. Key personnel are expected to be dedicated to this effort. For this key person, they shall have at a minimum, a bachelor's degree in computer science or related field.

##### **Program Manager**

Minimum Requirements: 11 Years of Experience and a bachelor's degree

- a) Organizes, directs, and manages contract operation support functions, involving multiple, complex and inter-related project tasks.
  - (b) Manages teams of contract support personnel at multiple locations.
  - (c) Maintains and manages the client interface at the senior levels of the client organization.
  - (d) Meets with customer and contractor personnel to formulate and review task plans and deliverable items.
- Ensures conformance with program task schedules and costs.

Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with

senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

**For IT Positions:**

- Baseline Certification
- Computing Environment Certification by date of award for all positions requiring elevated privileges

**7.11 Data Rights**

The Government requires unlimited rights in any technical data, software developed, and infrastructure designed first produced in the performance of this contract or any call order, in accordance with the FAR clause at 52.227-14 and DFARS 252.227-7014. In addition, for any technical data, software developed, and infrastructure designed first produced in the performance of a call order, the technical data, software developed, and infrastructure designed may be shared with other agencies or contractors during the period of performance of the call order, or after its termination. For any subcontractors or teaming partners, the Contractor shall ensure at proposal submission that the subcontractors and /or teaming partners are willing to provide the data rights required under the call order.

**8. QUALITY ASSURANCE**

**8.1 Performance Requirements Summary**

**8.1.1 Quality Assurance Surveillance Plan (QASP)**

The Government intends to utilize a Quality Assurance Surveillance Plan (QASP) to monitor the quality of the Contractor's performance. The oversight provided for in the contract and in the QASP will help to ensure that service levels reach and maintain the required levels throughout the contract term. Further, the QASP provides the GSA COR with a proactive way to avoid unacceptable or deficient performance and provides verifiable input for the required Contractor performance assessment. The QASP will be finalized immediately following award and a copy provided to the Contractor after award. The QASP is a living document and may be updated by the Government as necessary. The Government will also review the Monthly Status Report (MSR) and will attend regular work performance review meetings with the Contractor to survey quality of products and services.

The DMDC COR is responsible for the following:

- Reviewing and certifying Contractor invoices for accuracy and validity.
- Monitoring performance, reviewing, and approving task performance.
- Inspection and acceptance of deliverables.

The GSA COR, in collaboration with GSA Invoice Support Staff, will review the labor, travel, and ODC expenditures reflected in the Contractor invoices.

The GSA COR, in collaboration with GSA Invoice Support Staff, will ensure that the ceiling value and funded amount of the contract and task items are not exceeded in the areas of labor, travel, and ODCs.

The DMDC COR will provide surveillance for each PWS task, reviewing deliverables for conformance to requirements. Services, deliverables, and reports that conform to contract requirements will be accepted. The GSA COR will periodically consult with the DMDC COR concerning the acceptability of services. The DMDC COR will notify the Contractor in writing, or verbally when warranted, of the need for corrective action when work does not comply with the contract requirements. If corrective action does not result in conformance to requirements, the GSA COR or GSA CO will be apprised of items that remain at variance with requirements. The Government will document overall satisfaction with Contractor performance through completion of a Contractor Performance Assessment Report (CPAR)

routinely on an annual basis prior to exercising an option which will be uploaded into the Contractor Performance Assessment Reporting System at [www.cpars.gov](http://www.cpars.gov).

In accordance with the Quality Assurance Surveillance Plan, the Government will document overall satisfaction with Contractor performance through review and evaluation of the Contractor's success in meeting the standards and measures outlined in the performance metrics table included in the QASP.

#### **8.1.2 Performance Standards**

The Government will monitor the Contractor's performance in accordance with the Quality Assurance Surveillance Plan (QASP) described above and use the performance standards identified in the Performance Standards Metrics table to evaluate whether the Contractor's performance is satisfactorily meeting the standards specified in the Performance Requirements Summary (PRS) outlined in the QASP. The table identifies the incentives and disincentives, which will be applied to positive and negative past performance.

Past performance evaluations will be submitted to the Contractor Performance Assessment Reporting System (CPARS) for all government agencies to review. Past performance evaluations will contain narratives explaining reasons for positive and negative evaluations.

### **9. SECTION 508 REQUIREMENT**

The Contractor shall support and certify to the Government its compliance with Section 508 throughout the development and implementation of the work to be performed. They shall ensure only 508 compliant solutions are submitted. Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) requires that when Federal agencies develop, procure, maintain, or use electronic information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who do not have disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Applicable standards are 1194.21-1194-26. Additional Section 508 information can be found at the following websites:

<http://www.section508.gov/index.cfm?FuseAction=Content&ID=12>

<http://www.access-board.gov/508.htm>

<http://www.w3.org/WAI/Resources>

### **10. APPLICABLE DOCUMENTS AND DEFINITIONS**

#### **10.1 Compliance Documents**

The following documents provide specifications, standards, or guidelines that must be complied with to meet the requirements of this order:

- Please refer to the website which may be made through the TRICARE Management Activity Procurement Support (TPS) Website under tools and guides at [http://www.tricare.osd.mil/tps/Acquisition\\_Tools\\_Guides.cfm](http://www.tricare.osd.mil/tps/Acquisition_Tools_Guides.cfm)

#### **10.2 Reference Documents**

The following documents may be helpful to the Contractor in performing the work described in this document:

- Please refer to the website which may be made through the TRICARE Management Activity Procurement Support (TPS) Website under tools and guides at [http://www.tricare.osd.mil/tps/Acquisition\\_Tools\\_Guides.cfm](http://www.tricare.osd.mil/tps/Acquisition_Tools_Guides.cfm).
- DoD and VA policy such as the Department of Defense Manual for Written Material, VA Correspondence Manual

## 11.0 GSA INVOICING PROCEDURES

The following clauses are incorporated into the task or contract.

The Period of Performance (POP) for each invoice *shall* be for one calendar month. The contractor *shall* submit only one invoice per month per order/contract. The appropriate GSA office will receive the invoice by the twenty-fifth calendar day of the month after either:

- (1) The end of the invoiced month (*for services*) or
- (2) The end of the month in which the products (*commodities*) or deliverables (fixed-priced services) were delivered and accepted by the Government.

For Labor Hour and Time and Material orders/contracts each invoice shall show, the skill level category, the hours worked per skill level, the rate per skill level and the extended amount for that invoice period. It *shall* also show the total cumulative hours worked (inclusive of the current invoice period) per skill level, the hourly rate per skill level, the total cost per skill level, the total travel costs incurred and invoiced, and the total of any other costs incurred and invoiced, *as well as* the grand total of all costs incurred and invoiced.

For Labor Hour and Time and Material orders/contracts each invoice *shall clearly indicate* both the current invoice's monthly "burn rate" and the total average monthly "burn rate".

The contractor *shall submit* all required documentation (unless exempted by the contract or order) as follows:

For Travel: Submit the traveler's name, dates of travel, location of travel, and dollar amount of travel.

For ODCs: Submit a description of the ODC, quantity, unit price and total price of each ODC.

**Note:** The Government reserves the right to audit, thus; the contractor shall keep on file all backup support documentation for travel and ODCs.

**Note:** For Firm Fixed Price, Labor Hour, and Time and Material fiscal task items:

### Charges:

- All invoice charges must be task item specific (only one task item) unless concurrent task item periods of performance exist.



- For invoices with concurrent task item periods of performance all invoice charges must be service month specific (that is one service month only).

Credits:

- If the credit invoice is for the same year of a particular ACT#, the contractor shall include that credit on a subsequent invoice submission against that same ACT#. If the contractor is unwilling to offset a subsequent invoice then they must submit a refund check.
- When the credit invoice is for a different year, the contractor shall submit a refund check for that credit invoice.

Invoices that net to a credit balance **SHALL NOT** be accepted. Instead a refund check must be submitted by the contractor to GSA accordingly. The refund check shall cite the ACT Number, task item, and the period to which the credit pertains. The contractor shall provide the credit invoice as backup documentation. Do not attach credit invoice in ITSS or on the Finance website. It must be attached to the refund check. The refund check shall be mailed to:

General Services Administration

P.O. Box 979009  
St. Louis, MO 63101

**Posting Acceptance Documents:** Invoices shall be submitted monthly through GSA's electronic Web-Based Order Processing System, currently ITSS, to allow the client and GSA COTR to electronically accept and certify services received by the customer representative (CR). Included with the invoice will be all back-up documentation required such as, but not limited to, travel authorizations and training authorizations (including invoices for such).

**Receiving Agency's Acceptance:** The receiving agency has the following option in accepting and certifying services:

- a. Electronically: The client agency may accept and certify services electronically via GSA's electronic Web-Based Order Processing System, currently ITSS, by accepting the Acceptance Document generated by the contractor. Electronic acceptance of the invoice by the CR is considered concurrence and acceptance of services.

**Content of Invoice:** The contractor's invoice will be submitted monthly for work performed the prior month. The contractor may invoice only for the hours, travel and unique services ordered by GSA and actually used in direct support of the client representative's project. The invoice shall be submitted on official letterhead and shall include the following information at a minimum.

1. GSA Task Order Number
2. Task Order ACT Number

3. Remittance Address
4. Period of Performance for Billing Period
5. Point of Contact and Phone Number
6. Invoice Amount
7. Skill Level Name and Associated Skill Level Number
8. Actual Hours Worked During the Billing Period
9. Travel Itemized by Individual and Trip (if applicable)
10. Training Itemized by Individual and Purpose (if applicable)
11. Support Items Itemized by Specific Item and Amount (if applicable)

**Interim close outs:** The Government will close out each year of performance within 6 months of its expiration using the rates billed during that period. The contractor will be required to execute a waiver of claims to be included in a bi-lateral modification at the conclusion of the performance period.

**Final Invoice:** Invoices for the final performance period must be so identified and submitted within 6 months from completion. After this submission, no further charges are to be billed. A copy of the written client agency acceptance of task completion must be attached to the final invoice. If necessary, the contractor may request from GSA an extension for a final invoice that may exceed the 6-month time frame.

After the final invoice has been paid the contractor shall furnish a completed and signed Release of Claims (GSA Form 1142) to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

The Government reserves the right to require certification by a GSA COTR before payment is processed, *if necessary*.

#### **Close-out Procedures.**

**General:** The contractor shall submit a final invoice within sixty (60) calendar days after the end of the Performance Period. After the final invoice has been paid the contractor shall furnish a completed and signed Release of Claims (GSA Form 1142) to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

#### **Clause #2 - Acceptable Skill Level Variation in Severable Labor Hour and Time and Material Orders/Contracts (July/2005)**

The contractor may exceed the total number of *labor* hours per *awarded* skill level per base or option period, to a limit of 30% as long as the total task order *obligated* dollar amount per that base or option period is not exceeded, and *as* long as the contractor maintains an acceptable level of effort throughout the required period of performance.

*The contractor is not authorized to add new skill level categories or vary between levels within the same labor category without approval of the Government, formalized in a signed modification by the contracting officer.*

## 12. OTHER CLAUSES INCORPORATED INTO THIS CONTRACT

### 12.1 FAR Clauses: The following FAR clauses are included by reference:

- **Organizational Conflict of Interest (FAR 9.5)**
- **FAR 52.204-9 - Personal Identity Verification of Contractor Personnel. (Jan 2011).**
- **FAR 52.212-4 - Contract Terms and Conditions – Commercial Items, Alternate I (Dec 2014).**
- **FAR 52.217-5 - Evaluation of Options (Jul 1990)**
- **FAR 52.224-1 - Privacy Act Notification (Apr 1984)**
- **FAR 52.224-2 - Privacy Act (Apr 1984).**
- **FAR 52.227-14 - Rights in Data General (Dec 2007)**
- **FAR 52.232-18 - Availability of Funds (Apr 1984)**
- **FAR 52.232-20 - Limitation of Cost (APR 1984)**
- **FAR 52.232-22 - Limitation of Funds (APR 1984)**
- **FAR 52.232-25 - Prompt Payment**
- **FAR 52.222-54 - Employment Eligibility Verification (Jan 2009)**
- **FAR 52.227-16 - Additional Data Requirements (June 1987)**
- **FAR 52.232-19 - Availability of Funds for Next Fiscal Year (Apr 1984)**
- **FAR 52.239-1 - Privacy or Security Safeguards (Jul 2002)**
- **FAR 52.245-1 - Government Property (Aug 2010)**
- **FAR 52.246-6 - Inspection of Services-T&M and Labor Hour (Jan 1986)**
  
- **FAR 52.217-8 Option to Extend Services (NOV 1999)** - The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the contractor within 30 days of the end of the contract period of performance.
  
- **FAR 52.217-9 - Option to Extend the Term of the Contract (Mar 2000)** - The government may extend the term of this contract by written notice to the contractor within thirty (30) calendar days before the contract expires; provided that the government gives the contractor a preliminary written notice of its intent to extend at least forty-five (45) calendar days before the contract expires. The preliminary notice does not commit the government to an extension. If the government exercises this option, the extended contract shall be considered to include this option clause. The total duration of this contract, including the exercise of any options under this clause, shall not exceed three (3) years.
  
- **FAR 52.237-3 Continuity of Services (JAN 1991)**
  - (a) The contractor recognizes that the services under this contract are vital to the Government and must be continued without interruption and that, upon contract expiration, a successor, either the Government or another contractor, may continue them. The contractor agrees to—
    - (1) Furnish phase-in training; and
    - (2) Exercise its best efforts and cooperation to affect an orderly and efficient transition to a successor.
  - (b) The contractor shall, upon the Contracting Officer's written notice, (1) furnish phase-in, phase-out services for up to 90 days after this contract expires and (2) negotiate in good faith a plan with a successor to determine the nature and extent of phase-in, phase-out services required. The plan shall specify a training program and a date for transferring responsibilities for each division of work described in the plan and shall be subject to the Contracting Officer's approval. The contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the services

called for by this contract are maintained at the required level of proficiency.

(c) The contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this contract. The contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.

(d) The contractor shall be reimbursed for all reasonable phase-in, phase-out costs (*i.e.*, costs incurred within the agreed period after contract expiration that result from phase-in, phase-out operations) and a fee (profit) not to exceed a pro rata portion of the fee (profit) under this contract.

**12.2 DFARS Clauses:** The following DFARS clauses are in addition to those covered in the Alliant II contract:

- **DFARS 252.227-7015 - Technical Data – Commercial Items (JUN 2013)**
- **DFARS 252.209-7999 - REPRESENTATION BY CORPORATIONS REGARDING AN UNPAID DELINQUENT TAX LIABILITY OR A FELONY CONVICTION UNDER ANY FEDERAL LAW (DEVIATION 2014-00009) (FEB 2014)**

- **DFARS 252.232-7007 - LIMITATION OF GOVERNMENT'S OBLIGATION (MAY 2006)**

(a) Contract line item(s) \* through \* are incrementally funded. For these item(s), the sum of \$ \* of the total price is presently available for payment and allotted to this contract. An allotment schedule is set forth in paragraph (j) of this clause.

(b) For item(s) identified in paragraph (a) of this clause, the Contractor agrees to perform up to the point at which the total amount payable by the Government, including reimbursement in the event of termination of those item(s) for the Government's convenience, approximates the total amount currently allotted to the contract. The Contractor is not authorized to continue work on those item(s) beyond that point. The Government will not be obligated in any event to reimburse the Contractor in excess of the amount allotted to the contract for those item(s) regardless of anything to the contrary in the clause entitled "Termination for Convenience of the Government." As used in this clause, the total amount payable by the Government in the event of termination of applicable contract line item(s) for convenience includes costs, profit, and estimated termination settlement costs for those item(s).

(c) Notwithstanding the dates specified in the allotment schedule in paragraph (j) of this clause, the Contractor will notify the Contracting Officer in writing at least ninety days prior to the date when, in the Contractor's best judgment, the work will reach the point at which the total amount payable by the Government, including any cost for termination for convenience, will approximate 85 percent of the total amount then allotted to the contract for performance of the applicable item(s). The notification will state (1) the estimated date when that point will be reached and (2) an estimate of additional funding, if any, needed to continue performance of applicable line items up to the next scheduled date for allotment of funds identified in paragraph (j) of this clause, or to a mutually agreed upon substitute date. The notification will also advise the Contracting Officer of the estimated amount of additional funds that will be required for the timely performance of the item(s) funded pursuant to this clause, for a subsequent period as may be specified in the allotment schedule in paragraph (j) of this clause or otherwise agreed to by the parties. If after such notification additional funds are not allotted by the date identified in the Contractor's notification, or by an agreed substitute date, the Contracting Officer will terminate any item(s) for which additional funds have not been allotted, pursuant to the clause of this contract entitled "Termination for Convenience of the Government."

(d) When additional funds are allotted for continued performance of the contract line item(s) identified



in paragraph (a) of this clause, the parties will agree as to the period of contract performance which will be covered by the funds. The provisions of paragraphs (b) through (d) of this clause will apply in like manner to the additional allotted funds and agreed substitute date, and the contract will be modified accordingly.

(e) If, solely by reason of failure of the Government to allot additional funds, by the dates indicated below, in amounts sufficient for timely performance of the contract line item(s) identified in paragraph (a) of this clause, the Contractor incurs additional costs or is delayed in the performance of the work under this contract and if additional funds are allotted, an equitable adjustment will be made in the price or prices (including appropriate target, billing, and ceiling prices where applicable) of the item(s), or in the time of delivery, or both. Failure to agree to any such equitable adjustment hereunder will be a dispute concerning a question of fact within the meaning of the clause entitled "Disputes."

(f) The Government may at any time prior to termination allot additional funds for the performance of the contract line item(s) identified in paragraph (a) of this clause.

(g) The termination provisions of this clause do not limit the rights of the Government under the clause entitled "Default." The provisions of this clause are limited to the work and allotment of funds for the contract line item(s) set forth in paragraph (a) of this clause. This clause no longer applies once the contract is fully funded except with regard to the rights or obligations of the parties concerning equitable adjustments negotiated under paragraphs (d) and (e) of this clause.

(h) Nothing in this clause affects the right of the Government to terminate this contract pursuant to the clause of this contract entitled "Termination for Convenience of the Government."

(i) Nothing in this clause shall be construed as authorization of voluntary services whose acceptance is otherwise prohibited under 31 U.S.C. 1342.

(j) The parties contemplate that the Government will allot funds to this contract in accordance with the following schedule:

On execution of contract	\$ _____
(month) (day), (year)	\$ _____
(month) (day), (year)	\$ _____
(month) (day), (year)	\$ _____

-End of Clause-

### 13. SECURITY REQUIREMENTS

The Government requires the contractor to establish members of its workforce under this call are suitable for the job and are eligible for a Common Access Card (CAC) and public trust position at the appropriate level or security clearance prior to the call start date. The following Labor Categories **shall meet the current DMDC security standards for privileged access environments:**

- Program Manager
- Applications Systems Analyst (TS)
- Database Management Specialist (TS)

- Database Specialist (TS)
- Senior Developer
- Help Desk Technician

**The above personnel shall be vetted in JPAS and on board at award.**

#### **6.7.1 SECURITY CLEARANCE REQUIREMENTS**

Contractor personnel must be able to obtain and maintain the required access to classified information and the appropriate security clearance prior to beginning work on this call. The Government is not responsible for processing Contractor personnel for national security clearance (SECRET). The contractor shall comply with required DMDC personnel security requirements as specified by the Cybersecurity Branch. Interim Clearances will be reviewed upon notification to DMDC Information Security Branch. It is the responsibility of the contractor Facility Security Officer (FSO) to notify DMDC immediately if there is a change in clearance eligibility.

If at any time, any contractor's FSO is unable to obtain/maintain an adjudicated Personnel Security Investigation (PSI), the contractor shall immediately notify the DMDC Cybersecurity Branch and remove such person from work under this call. Overarching security requirements and Contractor access to classified information shall be as specified in the basic DD Form 254. All contractor personnel with access to unclassified information systems, including e-mail, shall have at a minimum a favorable T1. The contractor personnel shall have the required security clearance prior to arrival to perform the tasks of this call.

**Facility Security Clearance:** The work performed under this call is up to the Secret level and shall require Sensitive Compartmented Information (SCI) access eligibility for some personnel. The contractor shall have a final Secret Facility Clearance (FCL) from the Defense Security Service (DSS) Facility Clearance Branch (FCB).

**Security Clearance and Information Technology (IT) Level:** All personnel performing on this call shall be U.S. citizens.

**Investigation Requirements:** All personnel requiring Secret or IT-I eligibility under this call must undergo a favorably adjudicated Single Scope Background Investigation (SSBI) as a minimum investigation. The SSBI will be maintained current within 5-years and requests for Special Background Periodic Review (SBPR) will be initiated 90 days prior to the 5-year anniversary date of the previous SSBI or SBPR.

#### **6.7.2 CAC Requirements**

Contractor personnel with access to DMDC systems or data must comply with HSPD-12 Personal Identity Verification (PIV) issuance requirements, known as the Common Access Card (CAC) for DMDC and must be CAC or PIV ready prior to beginning work on this call:

- a) All Contractor personnel must obtain/maintain a favorable FBI National Criminal History Check (fingerprint check).
- b) Two forms of identity proofed identification (I-9 document).
- c) Be citizens of the United States.
- d) Submit a Standard Form (SF) 86 National Security Questionnaire through e-QIP that is favorably accepted by the Office of Personnel Management (OPM) for those:
  - a. Who do NOT have an active security clearance
  - b. Will be obtaining a position of trust through DMDC or
  - c. Have NOT been favorably adjudicated within the last 24 months.
- b) Background investigation has been scheduled by OPM.
- c) Maintain favorable FBI National Criminal History checks and ensure completion and successful adjudication as required for Federal employment.

### **6.7.3 Position of Trust**

All Contractor personnel with access to DMDC systems or data must comply with DoD Personnel Security Program. All persons on this call will be designated in a Critical-Sensitive, or Non-Critical Sensitive position (IT-I or IT-II) as determined by the Government per position responsibilities.

Prior to beginning work on this call, the contractor will complete all required personnel security requirements as specified by the Defense Human Resource Agency (DHRA), Personnel Security Office.

Complete and submit a vetting application (Standard Form (SF) 86 National Security Questionnaire through e-QIP, fingerprints and proof of US citizenship) that is favorably accepted by the Office of Personnel Management (OPM) for all employees under this call requesting a position of trust determination.

### **6.7.4 Security Clearance Requirements**

All Contractor personnel requiring access to classified information will need to obtain the appropriate security clearance prior to beginning work on this call. DHRA/DMDC is not responsible for processing contractor personnel for national security clearance (Secret SSBI). The contractor must comply with required DMDC personnel security requirements as specified by the Cybersecurity Division. Interim Clearances (e.g., Interim Secret) will be reviewed by DHRA Personnel Security Office. It is the responsibility of the contractor Facility Security Officer (FSO) to notify DHRA Personnel Security Office immediately if there is a change in clearance eligibility.

If at any time, any Contractor FSO is unable to obtain/maintain an adjudicated Personnel Security Investigation (PSI), the contractor shall immediately notify DHRA Personnel Security Office and DMDC Cybersecurity Division and remove such person from work under this call.

### **6.7.5 LAN Access Requirements:**

It is the responsibility of the contractor to comply with account access requirements as specified by the DMDC Cybersecurity Division.

- Standard User LAN access at a minimum requires:
  - a. Completed DMDC personnel security requirements.
  - b. Complete DD 2875 Form(s) for all access required.
  - c. Submit proof of completion for Personally Identifiable Information (PII) Training.
  - d. Submit proof of completion Cyber Awareness Challenge Training.
  - e. Adhere to and sign the DMDC Information Systems User Agreement(s).
- Privilege User LAN access at minimum requires:
  - a. Completed DMDC personnel security requirements.
  - b. Complete DD 2875 Form(s) for all access required.
  - c. Submit proof of completion Privilege User Cyber Awareness Challenge Training.
  - d. Adhere to and sign the DMDC Privilege Information Systems User Agreement(s).
  - e. DoD 8140.01, Cyberspace Workforce Management certification.
  - f. Computing Environment (CE) certification(s).

### **Cybersecurity Requirements**

**6.7.6.1** The contractor and all contractor personnel with access to or responsibility for non-public Government data under this call shall comply with DoD Instruction 8500.01 Cybersecurity, DoD Instruction 8510.01 Risk Management Framework, NIST SP 800-53 Cybersecurity Controls and Enhancements, DoD Directive 5400.11 DoD Privacy Program, DoD 6025.18-R DoD Health Information Privacy Regulation, DoD 5200.2-R Personnel Security Program, and Homeland Security Presidential Directive (HSPD) 12.

**6.7.6.2** The contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all nonpublic Government data to ensure the confidentiality, integrity, and availability of government data. At a minimum, this must include compliance with DoDI 8500.01, DoDI 8510.01 and NIST SP 800-53 and provisions for personnel security and the protection of sensitive information, including Personally Identifiable Information (PII).

**6.7.6.3** Contractor systems and information networks that receive, transmit, store, or process nonpublic government data must be accredited according to DoD Instruction 8510.01 Risk Management Framework (RMF) and comply with NIST SP 800-53 and annual Federal Information Security Management Act (FISMA) security control testing. All systems subject to RMF must present evidence of Assessment and Accreditation (A&A) testing in the form of an Authorization to Operate (ATO) and Cybersecurity Risk Assessment. Evidence of FISMA compliance must be presented in the form of a POA&M. The contractor will be responsible for the cost of Cybersecurity A&A and FISMA testing required for any Contractor owned and operated network, facility and/or application processing DoD information.



**6.7.6.4** The contractor shall ensure all media containing sensitive information (e.g., hard drives, removable disk drives, CDs, DVDs) considered for disposal will be destroyed. Prior to destruction, media will be sanitized, i.e., all prudent and necessary measures shall be taken to ensure data cannot be retrieved through known conventional or unconventional means. USB Flash drive use is prohibited by DoD.

**6.7.6.5** To the extent that the work under this call requires the contractor to have access to DoD sensitive information the contractor shall after receipt thereof, treat such information as confidential and safeguard such information from unauthorized use and disclosure. The contractor agrees not to appropriate such information for its own use or to disclose such information to third parties unless specifically authorized by the Government in writing.

**6.7.6.6** The contractor shall allow access only to those employees who need the sensitive information to perform services under this call and agrees that sensitive information shall be used solely for the purpose of performing services under this call. The contractor shall ensure that its employees will not discuss, divulge or disclose any such sensitive information to any person or entity except those persons within the Contractor's organization directly concerned with the performance of the call.

**6.8.6.7** The contractor shall report Cybersecurity incidents to the Cybersecurity Division.

**6.8.6.8** The contractor shall be responsible for safeguarding all government equipment, information and property provided for Contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.

**6.8.6.9** Contracting work performed shall be done using government provided email and resources. Resources include government furnished equipment. The contractor's company (and personal) computer shall not be used to perform to include store or transmit government work.

**6.8.6.10** Final approval for all Cybersecurity tasks under this call belongs to the Enterprise Service Directorate, Cybersecurity Division. The contractor is expected to obtain this final approval from Cybersecurity. All cybersecurity-related design, decisions, including cryptography, authentication, access control, data transfer and storage, Need-to-Know (NTK), or other IA technologies, must be coordinated with and approved by the Cybersecurity Division.

**6.8.6.11** The Government may terminate this call for default if Contractor or an employee of the contractor fails to comply with the provisions of this clause. The Government may also exercise any other rights and remedies provided by law or this call, including criminal and civil penalties.